(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 43 12 305 A 1**

(51) Int. Cl.[5]:
G 05 B 19/05

(21) Aktenzeichen: P 43 12 305.8
(22) Anmeldetag: 15. 4. 93
(43) Offenlegungstag: 27. 10. 94

DE 43 12 305 A1

(71) Anmelder:
ABB Patent GmbH, 68309 Mannheim, DE

(72) Erfinder:
Küber, Mathias, Dipl.-Ing., 6834 Ketsch, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:

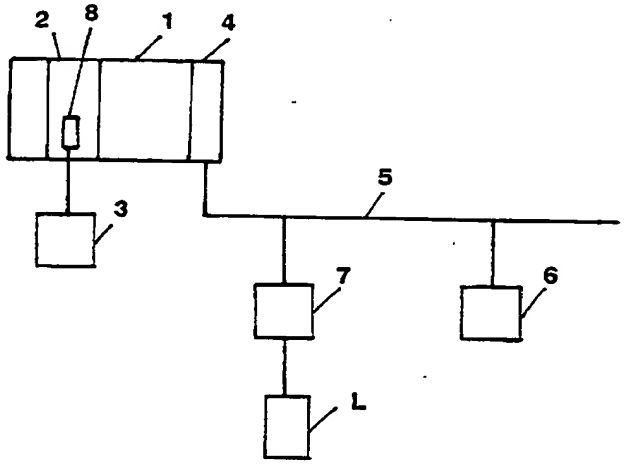
DE 40 32 033 C2
DE 39 19 558 C2
DE 33 02 223 A1
DE 32 23 946 A1

KIELHORN,Otto: Speicherprogrammierbare Steuerungen- Stand der Technik. In: etz, Bd.105,1984, H.11, S.534-538;
LEIST,K.: Sicherheitsgerichtete speicherprogram-mierbare Steuerungen. In: Automatisierungstechnische Praxis atp, Jg.29, H.6, 1987, S.267-275;
MÜLLER, Leo: Fehlererkennung bei der SPS-Program- mierung. In: der elektroniker, Nr.9/1987, S.40-45;
MÜLLER, L.: Wirkungsweise und Einsatz speicherpro-grammierbarer Steuerungen (III). In: de/der elek- tromeister + deutsches elektrohandwerk, 1981, H.13S.963-965;
KRÄMER,Manfred: Speicherprogrammierbare Steuerung für sicherheitstechnische Anwendungen. In: Energie& Automation 12,1990,H.5-6, S.8-11;
N.N.: Übernimmt Steuerungsaufgaben. In: elektro-technik, 69, H.12, 20.Aug.1987, S. 34-37;
N.N.: Erhöhte Verfügbarkeit von Prozeßsteuerungen.In: ABB Technik 8/9/89, S.31-35;
Jülly, U.: Sicherheitssteuerungen in vedrahtungs-programmierter und in speicherprogrammierter Ausführung. In: Automatisierungstechnische Praxis atp, 29.Jg., H.10/1987,S.470-474;
JÜLLY, U.: Funktionsweise und Programmierung einer speicherprogrammierten Sicherheitssteuerung. In: Automatisierungstechnische Praxis atp, 29.jg., H.11, 1987, S.532-534;

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Sicherheitsgerichtete speichergrogrammierbare Steuerung

(57) Mit der Erfindung wird vorgeschlagen, eine Standard-SPS (1) durch Ergänzungen zu einer sicherheitsgerichteten SPS zu ertüchtigen. Zu den Ergänzungen gehören spezielle sicherheitsgerichtete E/A-Geräte (7), die intern zweikanalig aufgebaut sind und selbsttätig sowohl einen Vergleichstest zwischen ihren Kanälen als auch zusätzliche Eigenüberwachungsfunktionen durchführen. Als weitere Ergänzung sind sicherheitsgerichtete Programm-Module im Anwenderprogramm der Zentraleinheit (2) der SPS (1) vorhanden, die eine redundante Überwachung der sicherheitsgerichteten E/A-Geräte (7) und eine Eigenüberwachung der Zentraleinheit (2) vornehmen. Die so gebildete sicherheitsgerichtete SPS ist geeignet zur Steuerung von Prozessen, die durch Abschalten in einen sicheren Zustand gebracht werden können.



DE 43 12 305 A1

Beschreibung

Die Erfindung bezieht sich auf eine speicherprogrammierbare Steuerung, die als sicherheitsgerichtete Steuerung ausgeführt ist. Solche, auch als fehlersichere Steuerungen bezeichnete Sicherheitssysteme finden im Rahmen von Prozeßanlagen Anwendung.

Es sind mehrere unterschiedliche Konzepte bekannt, mit denen Anforderungen an sicherheitsgerichtete Steuerungen entsprochen werden kann. Neben sicherheitstechnischen Anforderungen können mit solchen Konzepten auch Anforderungen an die Verfügbarkeit der Steuerungen erfüllt werden.

In Energie und Automation 12 (1990), Heft 5/6, Seite 8 bis 11 ist eine fehlersichere Steuerung beschrieben, die aus zwei vollständigen Standard-Automatisierungssystemen auf gebaut ist, und die hauptsächlich softwaremäßige Ergänzungen enthält. Der daraus bekannte prinzipielle Aufbau eines zweikanaligen Sicherheitssystems ist in **Fig.** 2 am Beispiel einer Anordnung mit einem binären Ausgang gezeigt. Man erkennt, daß bei einem solchen Konzept eine zu steuernde Last L über mehrere Leitungen D mit Ein- und Ausgabegeräte I, O der beiden Automatisierungssysteme A, B angeschlossen ist.

Die Zentraleinheiten C der beiden Systeme A, B sind miteinander gekoppelt.

Die vorgenannte Druckschrift enthält auch ein Verzeichnis mit Literaturquellen, denen die hier relevanten Begriffe aus der Sicherheitstechnik sowie deren Definition zu entnehmen sind.

Ein anderes Konzept ist aus der Druckschrift der Fa. Pepperl + Fuchs "FSC-System, Fail Safe Control System", Bestell-Nr. 16361 vom August 1991 bekannt. Das dort beschriebene System FSC-101 ist ein einkanaliges System, das bezüglich verschiedener Verfügbarkeitsstufen ausbaufähig ist. Das Grundsystem FSC-101 ist ein speziell als Sicherheitssystem entwickeltes Automatisierungssystem, dessen sämtliche Baugruppen als sicherheitsgerichtete Schaltkreise aufgebaut sind. Gegenüber einer Standard-SPS sind außerdem zusätzliche Module vorhanden, die allein im Hinblick auf sicherheitsgerichtete Systemeigenschaften erforderlich sind.

Den bekannten ein- oder zweikanaligen Sicherheitssystemen ist gemeinsam, daß sie einen hohen Geräteaufwand erfordern und relativ langsam arbeiten.

Die Erfindung bezieht sich auf Anwendungsfälle, in denen nur ein Teil der an das Steuerungssystem angeschlossenen Prozesse fehlersicher zu steuern sind und wobei diese Prozesse durch Abschalten in einen sicheren Zustand zu bringen sind. Solche Anwendungen sind z. B. gegeben bei Krananlagen, Feuerungsanlagen und Überwachungsanlagen. Es soll also ein sicherheitsgerichtetes, speicherprogrammierbares Steuerungssystem geschaffen werden, das nicht für Prozesse geeignet zu sein braucht, bei denen der sichere Zustand nicht durch Abschalten erreicht werden kann und bei denen es auf eine erhöhte Verfügbarkeit ankommt.

Diese Aufgabe wird gelöst durch eine im Patentanspruch 1 angegebene speicherprogrammierbare Steuerung mit nur einer Zentraleinheit und mehreren über wenigstens einen Buskoppler und wenigstens einen Eingabe/Ausgabe(E/A)-Bus anschließbaren E/A-Geräten, wobei alle diese Komponenten Bestandteile einer einkanaligen Standard-SPS sind, und wobei die SPS durch nachstehende Ergänzungen zu einer sicherheitsgerichteten SPS ertüchtigt ist:

a) an den E/A-Bus sind spezielle sicherheitsgerichtete E/A-Geräte anschließbar, die intern zweikanalig aufgebaut sind und selbsttätig einen Vergleichstest zwischen ihren Kanälen sowie zusätzliche Eigentests durchführen, und

b) die Zentraleinheit ist allein durch sicherheitsgerichtete Programm-Module ergänzt zur Durchführung sicherheitsgerichteter Funktionen, die sich auf sicherheitsgerichtete Anwenderfunktionen und zumindest auf eine zur Eigenüberwachung der sicherheitsgerichteten E/A-Geräte redundante Überwachung der sicherheitsgerichteten E/A-Geräte beziehen, sowie auf eine Selbstüberwachung der Zentraleinheit.

Das mit der erfindungsgemäßen Steuerung vorgestellte Konzept hat den Vorteil, daß auch eine schon vorhandene Standard-SPS nachträglich zur sicherheitsgerichteten speicherprogrammierbaren Steuerung ertüchtigt werden kann. Der nach außen hin einkanalige Aufbau erfordert keine besondere Außenverdrahtung. Durch die systemgemäße dezentrale Intelligenz wird erreicht, daß nur für den Anschluß der sicherheitsrelevanten Prozesse ein gegenüber Standard-Steuerungen erhöhter Aufwand notwendig ist. Die Anforderungen nach DIN V VDE 801 Anforderungsklasse 4 werden erfüllt.

Ausgestaltungen sind weiteren Patentansprüchen und der nachstehenden Beschreibung eines Ausführungsbeispiels zu entnehmen.

Fig. 1 zeigt eine erfindungsgemäße sicherheitsgerichtete SPS mit einkanaliger Systemstruktur. Diese ist aufgebaut aus einer Standard-SPS **1** mit einer Zentraleinheit **2**, die spezielle gespeicherte Programm-Module mit sicherheitsgerichteten Funktionen enthält und die mit Hilfe eines an eine Schnittstelle **8** anschließbaren Personal Computers **3** eingebbar sind. Die Standard-SPS enthält wenigstens einen Buskoppler **4**, an den ein E/A-Bus **5** angeschlossen ist. Der E/A-Bus ist im Ausführungsbeispiel eine Zweidraht-Kommunikationsverbindung. An den E/A-Bus **5** sind sowohl Standard-E/A-Geräte **6** als auch sicherheitsgerichtete E/A-Geräte **7** anschließbar. Die sicherheitsgerichteten E/A-Geräte **7** sind intern zweikanalig aufgebaut. Sicherheitsgerichtete Funktionen sind redundant überwacht, nämlich einmal durch Selbstüberwachungsmaßnahmen in den E/A-Geräten **7** und durch Funktionsüberwachung von der Zentrale **2** aus. Der Informationsaustausch zwischen E/A-Geräten **7** und der Zentrale **2** erfolgt unter Verwendung eines Sicherheitsprotokolls.

In den intern zweikanalig aufgebauten, sicherheitsgerichteten E/A-Geräten **7** wird durch Vergleichstests zwischen den beiden Kanälen, Selbsttests und Plausibilitätstest die erforderliche Sicherheit erreicht. Bei fehlender Übereinstimmung wird eine Ausgabe eines Schaltbefehls gesperrt. Darüber hinaus wird eine Fehlerdiagnose durch Überwachung auf Drahtbruch, Kurzschluß, Überspannung, Bereichsüberschreitung und weitere Fehlerarten durchgeführt.

In einer ausgeführten sicherheitsgerichteten SPS wird innerhalb einer spezifizierten Fehlertoleranzzeit von 100 Millisekunden jeder gefährliche Fehler erkannt und es wird eine Abschaltung in den sicheren Zustand durchgeführt.

Jeder einzeln an sich ungefährliche Fehler wird innerhalb einer Zweitfehlereintrittszeit von einer Stunde erkannt. Es wird dabei unterstellt, daß in dieser Zeit kein zweiter Fehler auftreten kann, der die Erkennung des

Fehlers verhindert.

Das Anwenderprogramm der Zentraleinheit enthält ein Programm-Modul das ausschließlich sicherheitsgerichtete Funktionen einschließlich der Überwachung der E/A-Geräte 7 bearbeitet. In diesem Programm-Modul werden nur Sicherheits-Verknüpfungselemente verwendet, die durch hochwertige Maßnahmen, z. B. durch redundante, diversitäre Programmierung gesichert sind. Außerdem werden Sicherheitsanforderungen an die Zentraleinheit durch eine besondere Behandlung sicherheitsrelevanter Betriebssystemaufrufe und durch Selbsttests erfüllt.

Mit der Verwendung von Sicherheits-Verknüpfungselementen wird erreicht, daß die Programmierung vom Anwender in üblicher Weise, also wie bei einer nicht sicherheitsgerichteten SPS, einfach ausgehend vom Funktionsplan, vorgenommen werden kann.

Da im Gesamtsystem sicherheits- und nicht sicherheitsgerichtete Systemkomponenten eingesetzt sind, muß eine Rückwirkungsfreiheit der nicht sicherheitsgerichteten Komponenten gegeben sein.

Patentansprüche

1. Speicherprogrammierbare Steuerung (SPS) mit nur einer Zentraleinheit (2) und mehreren über wenigstens einen Buskoppler (4) und wenigstens einen Eingabe/Ausgabe(E/A)-Bus (5) anschließbaren E/A-Geräten (6), wobei alle diese Komponenten (2, 4, 5, 6) Bestandteile einer einkanaligen Standard-SPS (1) sind, **dadurch gekennzeichnet,** daß die SPS (1) durch nachstehende Ergänzungen zu einer sicherheitsgerichteten SPS ertüchtigt ist:
   a) an den E/A-Bus (5) sind spezielle sicherheitsgerichtete E/A-Geräte (7) anschließbar, die intern zweikanalig aufgebaut sind und selbsttätig einen Vergleichstest zwischen ihren Kanälen sowie zusätzliche Eigentests durchführen, und
   b) die Zentraleinheit (2) ist allein durch sicherheitsgerichtete Programm-Module ergänzt zur Durchführung sicherheitsgerichteter Funktionen, die sich auf sicherheitsgerichtete Anwenderfunktionen und zumindest auf eine zur Eigenüberwachung der sicherheitsgerichteten E/A-Geräte (7) redundante Überwachung der sicherheitsgerichteten E/A-Geräte (7) beziehen, sowie auf eine Selbstüberwachung der Zentraleinheit (2).
2. Speicherprogrammierbare Steuerung nach Anspruch 1, dadurch gekennzeichnet, daß die Zentraleinheit (2) eine Schnittstelle (8) aufweist, an die ein Personal Computer (3) anschließbar ist, mit dessen Hilfe, die im Anwenderprogramm der Zentraleinheit (2) enthaltenen sicherheitsgerichtete Programm-Module ladbar sind, die durch redundante, diversitäre Programmierung gesichert sind.
3. Speicherprogrammierbare Steuerung nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die sicherheitsgerichteten E/A-Geräte (7) Mittel enthalten zur Durchführung von Plausibilitätstests.
4. Speicherprogrammierbare Steuerung nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß die Zentraleinheit (2) mit Hilfe der gespeicherten sicherheitsgerichteten Programm-Module neben gefährlichen Fehlern, die innerhalb einer spezifizierten Fehlertoleranzzeit zur Abschaltung in den sicheren Zustand führen, auch einzeln an sich ungefährliche Fehlern innerhalb einer spezifizierten Zweitfehlereintrittszeit erkennt und meldet.

Hierzu 1 Seite(n) Zeichnungen

Nummer: DE 43 12 305 A1
Int. Cl.[5]: G 05 B 19/05
Offenlegungstag: 27. Oktober 1994

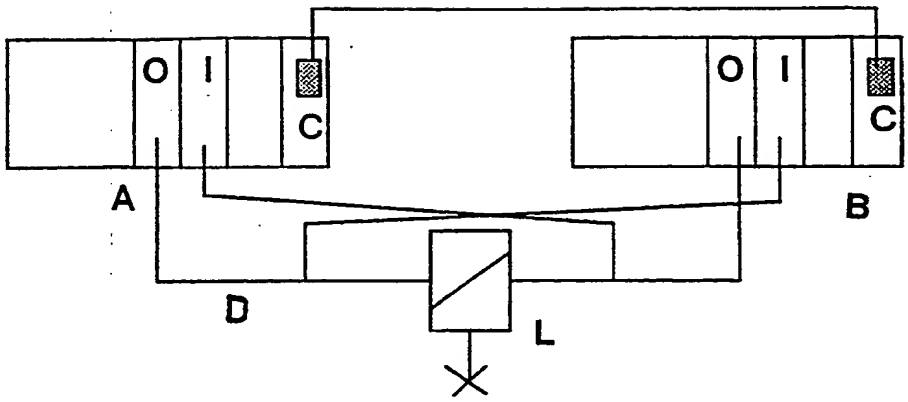


Fig. 2

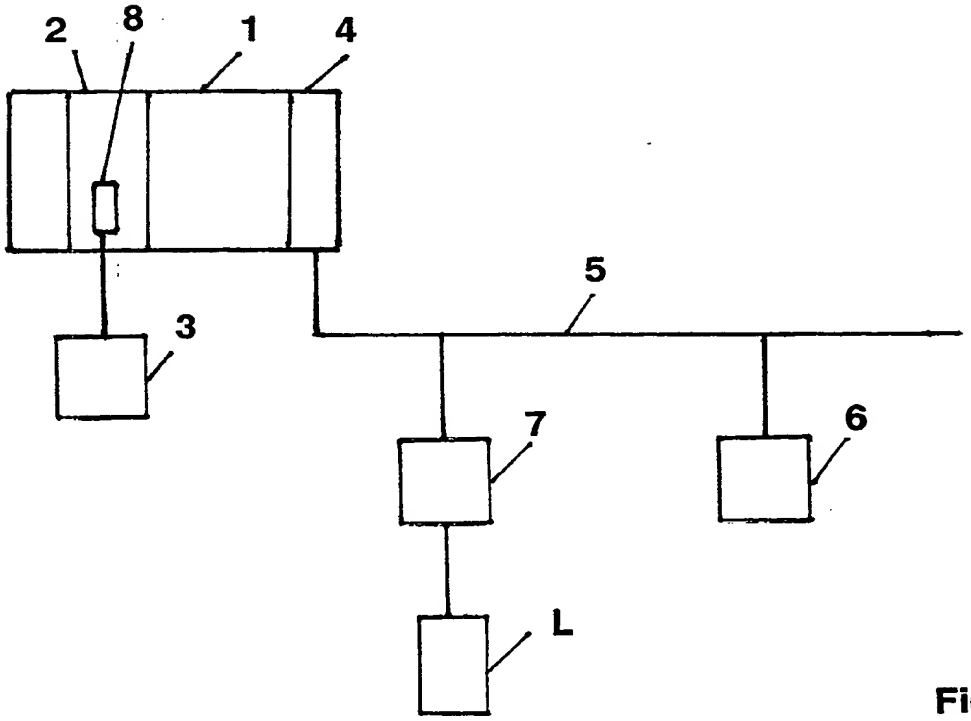


Fig. 1